USER GUIDE

Telstra

McAfee

PersonalFirewall Plus

Specifically tailored for Users of the BigPond Personal Firewall

McAfee SECURITY

BIGPOND

COPYRIGHT

TRADEMARK ATTRIBUTIONS

LICENSE AGREEMENT

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANIES YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEB SITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO NETWORK ASSOCIATES OR THE PLACE OF PURCHASE FOR A FULL REFUND.

CONTENTS

Getting Started 5

New Features 5
Documentation 6
System Requirements 6
Uninstalling Other Firewalls 7
Installing McAfee® Personal Firewall Plus™ 7
Testing McAfee® Personal Firewall Plus™ 9
Using McAfee® SecurityCenter™ 9

Using McAfee® Personal Firewall Plus™ 11

About the Summary 11
About Internet Applications 14
    Changing Permissions 15
    Changing Applications 16
About Inbound Events 16
    Understanding Events 17
        About IP Addresses 17
        Events from 0.0.0.0 18
        Events from 127.0.0.1 18
        Events from Computers on Your LAN 19
        Events from Private IP Addresses 19
    Showing Events in the Inbound Events Log 20
        Showing Today's Events 20
        Showing This Week's Events 20
        Showing the Complete Inbound Events Log 20
        Showing Only Events from the Selected Day 21
        Showing Only Events from the Selected Internet Address 21
        Showing Only Events with the Same Event Information 21
    Responding to Inbound Events 21
        Tracing the Selected Event 22
        Getting Advice from HackerWatch.org 22
        Reporting an Event 22

Signing Up for HackerWatch.org 22
Trusting an Address 23
Banning an Address 23
Managing the Inbound Events Log 24
Archiving the Inbound Events Log 24
Viewing Archived Inbound Events Log 25
Clearing the Inbound Events Log 25
Exporting Displayed Events 25
Copying an Event to the Clipboard 26
Deleting the Selected Event 26
About Alerts 26
Red Alerts 27
Green Alerts 27
Blue Alerts 27
Connection Attempt Blocked 28
Internet Application Blocked! 29
Application Wants to Access the Internet 30
Application Has Been Modified 31
Application Requests Server Access 32
Program Allowed to Access the Internet 33

Index 35

Welcome to McAfee Personal Firewall Plus!

McAfee Personal Firewall Plus software offers advanced protection for your computer and your personal data. Personal Firewall establishes a barrier between your computer and the Internet, silently monitoring Internet traffic for suspicious activities.

With it, you get the following features:

- Defends against potential hacker probes and attacks
- Complements anti-virus defenses
- Monitors Internet and network activity
- Alerts you to potentially hostile events
- Provides detailed information on suspicious Internet traffic
- Integrates Hackerwatch.org functionality, including event reporting, self-testing tools, and the ability to email reported events to other online authorities
- Provides detailed tracing and event research features

NEW FEATURES

- **Enhanced HackerWatch.org Integration**
  Reporting potential hackers is easier than ever. McAfee Personal Firewall Plus improves the functionality of HackerWatch.org, which includes event submission of potentially malicious events to the database.

- **Extended Intelligent Application Handling**
  When an application seeks Internet access, Personal Firewall first checks whether it recognizes the application as trusted or malicious. If the application is recognized as trusted, Personal Firewall automatically allows it access to the Internet so you do not have to. This database has been enhanced to provide users with more details about the applications connecting to the Internet.

- **Advanced Trojan Detection**
  McAfee Personal Firewall Plus combines application connection management with an enhanced database to detect and block more potentially malicious applications, such as Trojans, from accessing the Internet and potentially relaying your personal data.

- **Improved Visual Tracing**
  McAfee Personal Firewall Plus includes an updated intruder-tracing tool known as Visual Trace. Visual Trace includes easy-to-read graphical maps showing the originating source of hostile attacks and traffic worldwide, including detailed contact/owner information from originating IP addresses and all subsequent steps to your computer. McAfee Personal Firewall Plus has added more geographical data to the Visual Trace feature which enhances location details and provides more visual pin-pointed locations of intruders. Visual Trace allows users to visually track where intrusions originate, and with this new data, users are able to see a better graphical representation of their searches.

- **Improved Usability**
  McAfee Personal Firewall Plus includes a Setup Assistant and a User Tutorial to guide users in the setup and use of their firewall. Although the product is designed to use without any intervention, McAfee provides users with a wealth of resources to understand and appreciate what the firewall provides for them.

- **Improved Intrusion Prevention**
  McAfee Personal Firewall Plus protects your privacy more than ever by providing intrusion prevention of possible Internet threats. Using heuristic-like functionality, McAfee provides a tertiary layer of protection by blocking items that display symptoms of attacks or characteristics of hack attempts.

- **Enhanced Traffic Analysis**
  McAfee Personal Firewall Plus offers users a view of both incoming and outgoing data from their computers, as well as displaying application connections including applications that are actively "listening" for open connections. This allows users to see and act upon applications that might be open for intrusion.

DOCUMENTATION

Documentation for Personal Firewall Plus includes this user guide and an online Help file. The user guide is a subset of the online Help. For complete information and instructions on using Personal Firewall Plus, please refer to the online Help. After you install Personal Firewall Plus, you can access the online Help by opening Personal Firewall Plus, and then clicking the **Help** icon located in the top panel, or by clicking the **Help** button that appears on some dialog boxes.

SYSTEM REQUIREMENTS

- Microsoft® Windows 98, Windows Me, Windows 2000, or Windows XP
- Personal computer with 486 or higher processor (Pentium recommended)

- 8 MB of free hard disk space for installation
- Microsoft® Internet Explorer 5.01 or later

NOTE
To upgrade to the latest version of Internet Explorer, visit the Microsoft web site at http://www.microsoft.com/.

UNINSTALLING OTHER FIREWALLS

Before you install McAfee Personal Firewall Plus software, you must uninstall any other firewall programs on your computer. Please follow your firewall program's uninstall instructions to do so.

NOTE
If you use Windows XP, you do no need to disable the built-in firewall before installing McAfee Personal Firewall Plus software. However, we recommend that you do disable the built-in firewall. If you do not, you will not receive events in the Inbound Events log in McAfee Personal Firewall Plus.

INSTALLING MCAFEE® PERSONAL FIREWALL PLUS™

McAfee distributes McAfee Personal Firewall Plus software in two formats:

- On CD-ROM
- As a downloaded file from the McAfee web site

Personal Firewall Plus will be installed in the Program Files folder for McAfee. After you install and set up Personal Firewall Plus, you will be prompted to restart your computer. You must restart your computer before you can use Personal Firewall Plus.

To install Personal Firewall Plus:

1 If you downloaded Personal Firewall Plus from the McAfee web site, the Installation Wizard appears. Go to Step 2.

Or

If you purchased a Personal Firewall Plus CD, insert the Personal Firewall Plus software CD in your computer's CD-ROM drive. The License Agreement appears.

If the Installation Wizard does not automatically appear, the autorun feature on your computer might be disabled. Enable the autorun feature.

a. Select a country to indicated the language in which to view the License Agreement.

b. After you read the license agreement, click **Accept** to accept the terms of the agreement.

The McAfee Personal Firewall Plus Installation Wizard appears.

2 Follow the instructions on the Installation Wizard to complete the installation.

At the end installation, the Personal Firewall Plus Setup Assistant appears. (Figure 1-1).

Figure 1-1. Setup Assistant

Using the Setup Assistant

You are not required to use the Setup Assistant since Personal Firewall is already configured to start protecting your computer. The Setup Assistant helps you scan your computer for viruses and configure the following:

- Alert types you want to receive
- Your network connection type
- Application Recommendation settings

You can click **Cancel** anytime to accept the default settings. You can change Personal Firewall settings anytime.

NOTE
If you are upgrading to a new version of Personal Firewall, and you want to maintain your current Firewall settings, click **Cancel.**

After you use the Setup Assistant, you must restart your computer to complete the installation.

To use the Setup Assistant:

1. Click **Next.**
2. Follow the instructions on the dialog boxes that appear.
3. Click **Finish** when you are finished using the Setup Assistant.
4. You will be prompted to restart your computer. Click **OK** to restart your computer now, or click **Cancel** to restart your computer later. You must restart your computer before you can use Personal Firewall.

TESTING MCAFEE® PERSONAL FIREWALL PLUS™

To test Personal Firewall:

1. Right-click the McAfee icon  , point to **Personal Firewall**, and then click **Test Firewall.**
2. Personal Firewall opens Internet Explorer and goes to http://www.hackerwatch.org/, a web site maintained by McAfee Security. Please follow the directions on the Hackerwatch.org Probe page to test Personal Firewall.

NOTE
If you connect to the Internet through a proxy server or Network Address Translation server, as is the case in most office networks (LANs), you will not get a proper reading. Hackerwatch.org's firewall tester looks for which computer asked for the firewall test and tests that computer. If you connect through a proxy or NAT server, it simply relays your computer's request for the firewall test, and Hackerwatch.org will test the wrong computer. The results that you get belong to the proxy server—not to your computer.

USING MCAFEE® SECURITYCENTER™

McAfee SecurityCenter is your one-stop security shop, accessible from its icon in your Windows system tray or from your Windows desktop. With it, you can perform these useful tasks:

- Get free security analysis for your computer.
- Launch, manage, and configure all your McAfee subscriptions from one icon.
- See continuously updated virus alerts and the latest product information.

- Receive free trial subscriptions to download and install trial versions directly from McAfee using our patented software delivery process.
- Get quick links to frequently asked questions and account details at the McAfee web site.

> **NOTE**
> For more information about its features, please click **Help** in the SecurityCenter dialog box.

While SecurityCenter is running and all of the McAfee features installed on your computer are enabled, a red M icon  appears in the Windows system tray. This area is usually in the lower-right corner of the Windows desktop and contains the clock.

If one or more of the McAfee applications installed on your computer are disabled, the McAfee icon changes to black  .

To open McAfee SecurityCenter:

1. Right-click the McAfee icon  .
2. Click **Open SecurityCenter**.

To access a McAfee Personal Firewall Plus feature:

1. Right-click the McAfee icon  .
2. Point to **Personal Firewall**, and then click the feature you want to use.

To open Personal Firewall:

Right-click the McAfee icon, point to **Personal Firewall**, and click **View Summary**, **Internet Applications, Inbound Events,** or **Utilities**.

ABOUT THE SUMMARY

The Personal Firewall Summary includes four summary pages: Main Summary, Application Summary, Event Summary, and HackerWatch Summary. The Summary pages contain a variety of reports on recent inbound events, application status, and world-wide intrusion activity reported by HackerWatch.org. You will also find links to common tasks performed in Personal Firewall.

To open the Personal Firewall Summary pages, right-click the McAfee icon, point to **Personal Firewall**, and then click **View Summary**. The Main Summary page appears (Figure 2-2).

Figure 2-2. Main Summary page

Click the following to navigate to different Summary pages:

Item	Description
Change View	Click **Change View** to open a list of Summary pages. From the list, select a Summary page to view.
Right arrow 	Click the right arrow icon to view the next Summary page.
Left arrow 	Click the left arrow icon to view the previous Summary page.
Home 	Click the home icon to return to the **Main Summary** page.

The Main Summary page provides the following information:

Item	Description
Security Setting	The security setting status tells you the level of security at which the firewall is set. Click the link to change the security level.
Blocked Events	The blocked events status displays the number of events that have been blocked today. Click the link to view event details from the Inbound Event page.
Application Rule Changes	The application rule status displays the number of application rules that have been changed recently. Click the link to view the list of allowed and blocked applications and to modify application permissions.
What's New?	**What's New?** shows the latest application that was granted full access to the Internet.
Last Event	**Last Event** shows the latest inbound events. You can click a link to trace the event or to trust the IP address. Trusting an IP address allows all traffic from the IP address to reach your computer.
Daily Report	**Daily Report** displays the number of inbound events that Personal Firewall blocked today, this week, and this month. Click the link to view event details from the Inbound Event page.
Active Applications	**Active Applications** displays the applications that are currently running on your computer and accessing the Internet. Click an application to view which IP addresses the application is connecting to.
Common Tasks	Click a link in **Common Tasks** to go to Personal Firewall pages where you can view firewall activity and perform tasks.

To view the Application Summary page, click **Change View**, and then select **Application Summary**. The Application Summary page provides the following information:

Item	Description
Traffic Monitor	The **Traffic Monitor** shows inbound and outbound traffic volume across your Internet connection in the last ten minutes. Click the graph to view traffic monitoring details.
Active Applications	**Active Applications** shows the bandwidth usage of your computer's most active applications during the last 24 hours. **Application** — The application accessing the Internet. **%** — The percentage of bandwidth used by the application. **Permission** — The type of Internet access the application is allowed. **Rule Created** — When the application rule was created.
What's New?	**What's New?** shows the latest application that was granted full access to the Internet.
Active Applications	**Active Applications** displays the applications that are currently running on your computer and accessing the Internet. Click an application to view which IP addresses the application is connecting to.
Common Tasks	Click a link in **Common Tasks** to go to Personal Firewall pages where you can view application status and perform application-related tasks.

To view the Event Summary page, click **Change View**, and then select **Event Summary**. The Event Summary page provides the following information:

Item	Description
Port Comparison	**Port Comparison** shows a pie chart of the most frequently attempted ports on your computer during the past 30 days. You can click a port name to view details from the Inbound Events page. You can also move your mouse pointer over the port number to see a description of the port.
Top Offenders	**Top Offenders** shows the most frequently blocked IP addresses, when the last inbound event occurred for each address, and the total number of inbound events in the past thirty days for each address. Click an event to view event details from the Inbound Events page.
Daily Report	**Daily Report** displays the number of inbound events that Personal Firewall blocked today, this week, and this month. Click a number to view the event details from the Inbound Events log.

Item	Description
Last Event	**Last Event** shows the latest inbound events. You can click a link to trace the event or to trust the IP address. Trusting an IP address allows all traffic from the IP address to reach your computer.
Common Tasks	Click a link in **Common Tasks** to go to Personal Firewall pages where you can view details of events and perform event-related tasks.

To view the HackerWatch Summary page, click **Change View**, and then select **HackerWatch Summary**. The HackerWatch Summary page provides the following information:

Item	Description
World Activity	**World Activity** shows a world map identifying recently blocked activity monitored by HackerWatch.org. Click the map to open the Global Threat Analysis Map in HackerWatch.org.
Event Volume	**Event Volume** shows the number of inbound events submitted to HackerWatch.org.
Global Port Activity	**Global Port Activity** shows the top ports, in the past 5 days, that appear to be threats. Click a port to view the port number and port description.
Common Tasks	Click a link in **Common Tasks** to go to HackerWatch.org pages where you can get more information on world-wide hacker activity.

ABOUT INTERNET APPLICATIONS

Use the Internet Applications page to view the list of allowed and blocked applications.

Right-click the McAfee icon, point to **Personal Firewall,** and then click **Internet Applications**. The Internet Applications page appears (Figure 2-3).

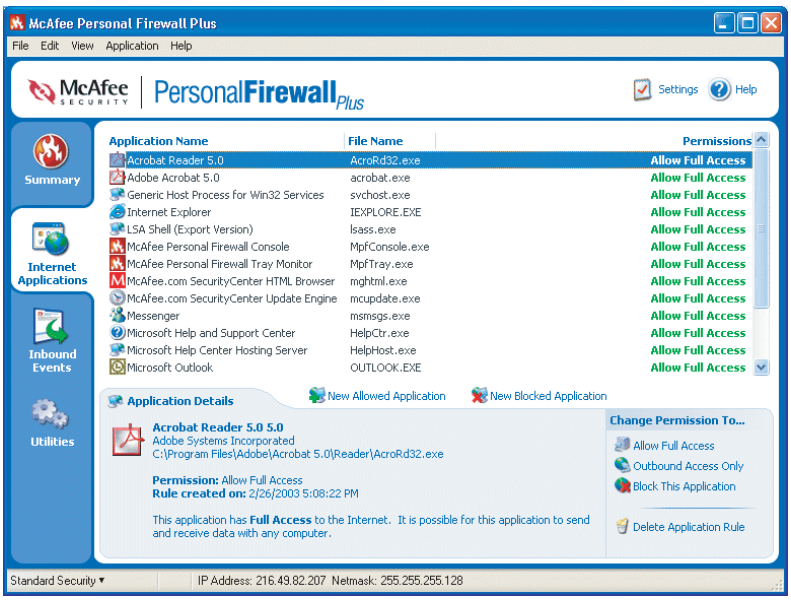

Figure 2-3. Internet Applications page

The Internet Applications page provides the following information:

- Application names
- File names
- Current permission levels
- Application details: pathnames, permission timestamps, and explanations of permission types

Changing Permissions

Personal Firewall lets you set the permission level for each application that requests Internet access.

To change a permission level:

1. Right-click the McAfee icon, point to **Personal Firewall,** and then click **Internet Applications**.

2. In the **Permissions** list, right-click the permission level for an application, and choose a different level:

   - Click **Allow Full Access** to allow the application to both send and receive data.

- Click **Outbound Access Only** to prevent the application from receiving data.
- Click **Block This Application** to prevent the application from sending or receiving data.

To delete a permission level:

1. Right-click the McAfee icon, point to **Personal Firewall,** and then click **Internet Applications**.
2. In the **Permissions** list, right-click the permission level for an application, and click **Delete Application Rule**.

The next time the application requests Internet access, you can set its permission level to re-add it to the list.

Changing Applications

To change the list of allowed and blocked Internet applications:

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **Internet Applications**.
2. Add or remove applications from the **Application Name** list:

   - To add a new “Allowed” application, click **New Allowed Application**, select the application to allow, and then click **Open.**
   - To add a new “Blocked” application, click **New Blocked Application**, select the application to block, and then click **Open**.
   - To remove an application from the list, click **Delete Application Rule**.

ABOUT INBOUND EVENTS

Use the Inbound Events page to view the Inbound Events log generated when Personal Firewall blocks unsolicited Internet traffic.

Right-click the McAfee icon, point to **Personal Firewall**, and then click **Inbound Events**. The Inbound Events page appears (Figure 2-4).

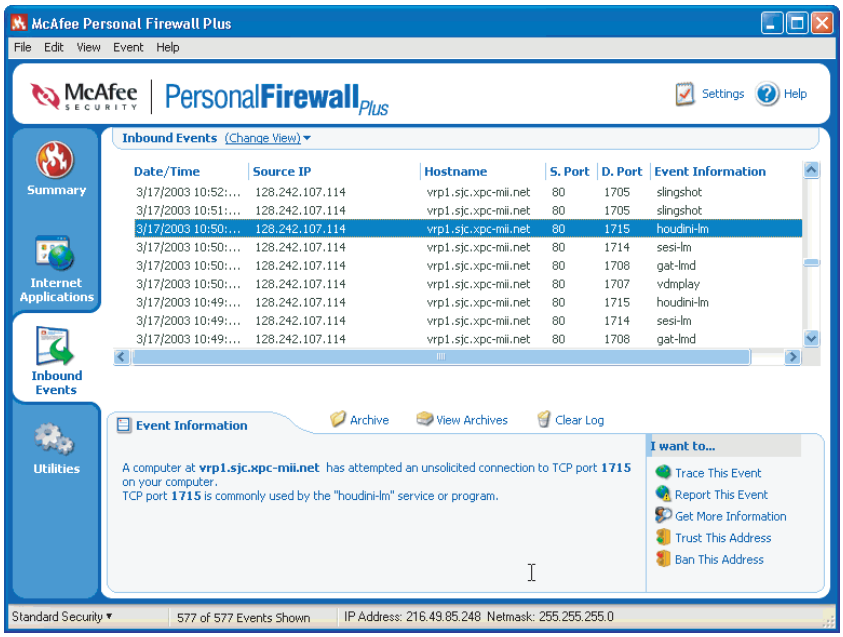

Figure 2-4. Inbound Events page

The Inbound Events page provides the following information:

- Timestamps
- Source IPs
- Hostnames
- Service or application names
- Event details: connection types, connection ports, and explanations of port events

Understanding Events

About IP Addresses

IP addresses are numbers: four numbers each between 0 and 255 to be precise. These numbers identify a specific place that traffic can be directed to on the Internet.

Special IP Addresses

Several IP addresses are unusual for various reasons:

Non-routable IP addresses — These are also referred to as "Private IP Space." These IP addresses cannot be used on the Internet. Private IP blocks are 10.x.x.x, 172.16.x.x - 172.31.x.x, and 192.168.x.x.

Loop-back IP addresses — Loop-back addresses are used for testing purposes. Traffic sent to this block of IP addresses comes right back to the device generating the packet. It never leaves the device, and is primarily used for hardware and software testing. The Loop-Back IP block is 127.x.x.x.

Null IP address — This is an invalid address. When it is seen, it indicates that the traffic had a blank IP address. This is obviously not normal, and frequently it indicates that the sender is deliberately obscuring the origin of the traffic. The sender will not be able to receive any replies to their traffic unless the packet is received by an application that understands the contents of the packet that will include instructions specific to that application. Any address that starts with 0 (0.x.x.x) is a null address. For example, 0.0.0.0 is a null IP address.

Events from 0.0.0.0

If you see events from IP address 0.0.0.0, there are two likely causes. The first, and most common, is that for some reason your computer received a badly formed packet. The Internet isn't always 100% reliable, and bad packets can occur. Since Personal Firewall sees the packets before TCP/IP can validate them, it might report these packets as an event.

The other situation occurs when the source IP is spoofed, or faked. Spoofed packets might be a sign that someone is scanning around looking for Trojans, and they happened to try your computer. It's important to remember that Personal Firewall blocked this attempt, so your computer is safe.

Events from 127.0.0.1

Events will sometimes list their source IP as 127.0.0.1. It's important to note that this IP is special, and is referred to as the loopback address.

Basically, no matter what computer you're on, 127.0.0.1 always refers to yourself. This address is also referred to as localhost, as the computer name localhost will always resolve back to the IP address 127.0.0.1.

Does this mean that your computer is attempting to hack itself? Is some Trojan or spyware taking over your computer? Not likely. Many legitimate programs use the loopback address for communication between components. For example, many personal mail or web servers let you configure them via a web interface that is usually accessible through something like http://localhost/.

However, Personal Firewall allows traffic from these programs, so if you see events from 127.0.0.1, it most likely means that the source IP address is spoofed, or faked. Spoofed packets are usually signs of someone scanning for Trojans. It's important to remember that Personal Firewall blocked this attempt, so your computer is safe. Obviously, reporting events from 127.0.0.1 won't do any good, so there's no need to do so.

With that said, there are some programs, most notably Netscape 6.2 and higher, that requires you to add 127.0.0.1 to the trusted IP list. These programs' components communicate between each other in such a manner that Personal Firewall cannot determine if the traffic is local or not.

In the example of Netscape 6.2, if you do not trust 127.0.0.1, then you will not be able to use your buddy list. Therefore, if you see traffic from 127.0.0.1 and all of the applications on your computer work normally, then it is safe to block this traffic. However, if a program (like Netscape) is having problems, place 127.0.0.1 in the Trusted IP Addresses list in Personal Firewall, and then find out if the problem is resolved.

If placing 127.0.0.1 in the trusted IP list fixes the problem, then you need to weigh your options: if you trust 127.0.0.1, your program will work, but you will be more open to spoofed attacks. If you do not trust the address, then your program will not work, but you will remain protected against such malicious traffic.

Events from Computers on Your LAN

Events can be generated from computers on your local area network (LAN). To show that these events are coming from somewhere "close to home," Personal Firewall displays them in green.

In most corporate LAN settings, you'll want to check "Make all computers on your LAN Trusted" in the Trusted IP Addresses options.

However, it's important to note that in some situations, your 'local' network can be as dangerous, or even more dangerous, than the outside network. This is especially true if you are on a high-bandwidth public network, such as DSL or cable modems. In such a scenario, it's best not to check the "Make all computers on your LAN Trusted" option.

If you are on a home network connected to broadband, you should instead manually add the IP addresses of your local computers to the Trusted IP list. Remember, you can use .255 style addresses to trust an entire block. For example, you can trust your entire ICS (Internet Connection Sharing) network by trusting the IP 192.168.255.255.

Events from Private IP Addresses

IP addresses of the format 192.168.xxx.xxx, 10.xxx.xxx.xxx, and 172.16.0.0 - 172.31.255.255 are referred to as non-routable or private IP addresses. These IP addresses should never leave your network, and can be trusted most of the time.

The 192.168 block is used with Microsoft Internet Connection Sharing (ICS). If you are using ICS, and see events from this IP block, you might want to add the IP address 192.168.255.255 to your trusted IP list. This will trust the entire 192.168.xxx.xxx block.

If you are not on a private network, and see events from these IP ranges, the source IP address might be spoofed, or faked. Spoofed packets are usually signs that someone is scanning for Trojans. It's important to remember that Personal Firewall blocked this attempt, so your computer is safe.

Since private IP addresses refer to different computers depending on what network you are on, reporting these events will have no effect, so there's no need to do so.

Showing Events in the Inbound Events Log

The Inbound Events log allows you to conveniently display events in a number of ways. The default view limits the view to events occurring on the current day. You can also view events that occurred during the past week, or view the complete log.

Personal Firewall also lets you display inbound events from specific days, from specific Internet addresses (IP addresses), or events that contain the same event information.

For information about an event, click the event, and the information appears in the **Event Information** area at the bottom of the Inbound Events page.

Showing Today's Events

To show only events occurring today:

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **Inbound Events**.

2. From the **View** menu, click **Show Today's Events**. The Inbound Events log displays events occurring today only.

Showing This Week's Events

To show events occurring in the past week:

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **Inbound Events**.

2. From the **View** menu, click **Show This Week's Events.** The Inbound Events log displays events occurring this week only.

Showing the Complete Inbound Events Log

To show all of the events in the Inbound Events log:

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **Inbound Events.**

1 From the **View** menu, click **Show Complete Log.**

2 The Inbound Events log displays all events, not including archives, from the Inbound Events log.

Showing Only Events from the Selected Day

This is useful when you just want to look at events from a specific day. All events not occurring on that day are hidden.

1 Right-click the McAfee icon, point to **Personal Firewall**, and click **Inbound Events**.

2 From the **View** menu, click **Show Only Events from Selected Day**.
Today's events appear on the Inbound Events log.

Showing Only Events from the Selected Internet Address

This is useful when you need to see other events originating from a specific Internet address. All other events are hidden.

1 Right-click the McAfee icon, point to **Personal Firewall**, and click **Inbound Events**.

2 From the **View** menu, click **Show Only Events from Selected Internet Address**.
Events originating from the selected Internet address appear in the Inbound Events log.

Showing Only Events with the Same Event Information

This is useful when you need to see if there are other events in the Inbound Events log that have the same information in the Event Information column as the event you selected. You can find out how many times this happened, and if it is from the same source. The Event Information column provides a description of the event and, if known, the common program or service that uses that port.

1 Right-click the McAfee icon, point to **Personal Firewall**, and click **Inbound Events**.

2 From the **View** menu, click **Show Only Events with the Same Event Information**.
Events with the same Event Information appear in the Inbound Events log.

Responding to Inbound Events

In addition to getting details about events in the Inbound Events log, you can try to perform a Visual Trace of the IP addresses for an event in the Inbound Events log, or get event details at the anti-hacker online community HackerWatch.org web site.

Tracing the Selected Event

You can try to perform a Visual Trace of the IP addresses for an event in the Inbound Events log.

1. Right-click the McAfee icon, point to **Personal Firewall**, and click **Inbound Events.**
2. Right-click the event you want to trace, and then click **Trace Selected Event.**
3. You can also double click an event to perform a trace.
4. By default, Personal Firewall begins a Visual Trace using the integrated Visual Trace program.

Getting Advice from HackerWatch.org

You can get more information about an event from the anti-hacker online community HackerWatch.org by doing the following:

1. Right-click the McAfee icon, point to **Personal Firewall**, and click **Inbound Events.**
2. Locate and click the event about which you want more information.
3. From the **Event** menu, click **More Information on Event.**

Your web browser opens and goes to the HackerWatch.org web site at http://www.hackerwatch.org/ to get details about the event type and advice about whether to report the event.

Reporting an Event

To report an event that you think was an attack on your computer, please do the following:

1. Right-click the McAfee icon, point to **Personal Firewall**, and click **Inbound Events.**
2. Click the event you want to report, and then click **Report This Event** in the lower right pane.
3. Personal Firewall reports the event to the HackerWatch.org web site using your unique ID.

Signing Up for HackerWatch.org

When you first open the Summary page, Personal Firewall contacts HackerWatch.org to generate your unique user ID. If you are an existing user, your sign-up is automatically validated. If you are a new user, you must enter a nickname and email address, and then click the validation link in the confirmation email from HackerWatch.org to be able to use the event filtering/emailing features at its web site.

You can report events to HackerWatch.org without validating your user ID. However, to filter events and email events to a friend, you must sign up for the service.

Signing up for the service allows your submissions to be tracked and lets us notify you if HackerWatch.org needs more information or further action from you. We also require you to sign up because we must confirm any information we receive for that information to be useful.

All email addresses provided to HackerWatch.org are kept confidential. If a request for additional information is made by an ISP, that request is routed through HackerWatch.org; your email address is never exposed.

Trusting an Address

If you see an event in the Inbound Events log that contains an IP address that you need to allow, you can have Personal Firewall allow connections from it at all times:

1. Right-click the McAfee icon, point to **Personal Firewall**, and click **Inbound Events**.
2. Right-click the event whose IP address you want trusted, and click **Trust the Source IP Address.**
3. Verify that the IP address displayed in the Trust This Address confirmation message is correct, and click **OK**.

   The IP address is added to the Trusted IP Addresses list.

To verify that the IP address was added:

1. Click the **Utilities** tab.
2. Click the **Trusted & Banned IPs** icon, and then click the **Trusted IP Addresses** tab.

   The IP address will be in the **Trusted IP Addresses** list.

Banning an Address

If an IP address appears in your Inbound Events log, this indicates that traffic from that address was blocked. Therefore, banning an address adds no additional protection unless your computer has ports that are deliberately opened through the System Services feature, or unless your computer has an application that has permission to receive traffic.

Add an IP address to your banned list only if you have one or more ports that are deliberately open and if you have reason to believe that you must block that address from accessing the open port(s).

If you see an event in the Inbound Events log that contains an IP address that you want to ban, you can have Personal Firewall prevent connections from it at all times:

1 Right-click the McAfee icon, point to **Personal Firewall**, and click **Inbound Events**.

2 Right-click the event whose IP address you want to ban, and click **Ban the Source IP Address.**

3 Verify that the IP address displayed in the Ban This Address confirmation message is correct, and click **OK.**

The IP address is added to the Banned IP Addresses list.

To verify that the IP address was added:

1 Click the **Utilities** tab.

2 Click the **Trusted & Banned IPs** icon, and then click the **Banned IP Addresses** tab.

The IP address appears in the Banned IP Addresses list.

Managing the Inbound Events Log

You can use the Inbound Events page to manage the events in the Inbound Events log generated when Personal Firewall blocks unsolicited Internet traffic.

Archiving the Inbound Events Log

You can archive the current Inbound Events log in a file on your hard drive. We recommend that you archive your event log periodically because the event log can get quite large.

To archive the Inbound Events Log:

1 Right-click the McAfee icon, point to **Personal Firewall**, and click **Inbound Events**.

2 From the **File** menu, click **Archive Log.**

3 Click **Yes** on the confirmation message.

4 Click **Save** to save the archive in the default location, or browse to a location where you want to save the archive.

Viewing Archived Inbound Events Log

You can view any Inbound Events log that you previously archived.

> **WARNING**
> Before you view your archives, you must archive your current Inbound Events log. Failure to do so will clear your current Inbound Events log when you view an archive.

1. Right-click the McAfee icon, point to **Personal Firewall,** and click **Inbound Events**.
2. From the **File** menu, click **View Archived Logs.**
3. Click the archive file name (you might have to browse to it) and click **Open.**
   The archived data appears in the Inbound Events log.

Clearing the Inbound Events Log

You can clear all information from the Inbound Events log.

> **WARNING**
> Once you clear the Inbound Events log, you cannot recover it. If you think you will need the event log in the future, you should archive it instead.

1. Right-click the McAfee icon, point to **Personal Firewall,** and click **Inbound Events**.
2. From the **File** menu, click **Clear Log.**
3. Click **Yes** on the confirmation box to clear the log.
   The Event Log is now empty.

Exporting Displayed Events

You can export your event log to a text file in case you need to share it with your ISP, technical support, or law enforcement officials.

1. Right-click the McAfee icon, point to **Personal Firewall,** and click **Inbound Events**.
2. From the **File** menu, click **Export Displayed Events.**
3. Browse to the location to which you want to save the events.
4. Rename the file if necessary, and then click **Save**.
   Your events are saved to a .txt file in the location you chose.

Copying an Event to the Clipboard

You can copy an event to the clipboard so that you can paste it in a text file using Notepad.

1. Right-click the McAfee icon, point to **Personal Firewall**, and click **Inbound Events**.
2. Click the event in the Inbound Events log that you need to export.
3. From the **Edit** menu, click **Copy Selected Event to Clipboard.**
4. Open Notepad: Click the Windows Start button, point to Programs, then Accessories, and then click Notepad.
5. From the **Edit** menu, click **Paste**. The event appears in Notepad. Repeat this step until you have all of the necessary events.
6. Save the Notepad file in a safe place.

Deleting the Selected Event

You can delete events from the Inbound Events log.

1. Right-click the McAfee icon, point to **Personal Firewall**, and click **Inbound Events**.
2. Click the event in the Inbound Events log that you want to delete.
3. From the **Edit** menu, click **Delete Selected Event**.
   The event is deleted from the Inbound Events log.

ABOUT ALERTS

We strongly recommend that you become familiar with the types of alerts you will encounter while using Personal Firewall. Review the following types of alerts that can appear and the possible responses you can choose, so that you can confidently respond to an alert.

NOTE
Recommendations on alerts help you decide how to handle an alert. For recommendations to appear on alerts, click the **Utilities** tab, click the **Alert Settings** icon, and then select either **Use Smart Recommendations** (the default) or **Display Smart Recommendations only** from the **Smart Recommendations** list.

Red Alerts

Red alerts contain important information that requires your immediate attention. Red alerts are as follows:

- **Internet Application Blocked!** — This alert appears if Personal Firewall blocks an application from accessing the Internet. For example, if a Trojan program alert appears, McAfee automatically denies this program access to the Internet and recommends that you scan your computer for viruses.
- **Application Wants to Access the Internet** — This alert appears when Personal Firewall detects Internet or network traffic for new applications. (Standard or Tight Security)
- **Application Has Been Modified** — This alert appears when Personal Firewall detects that an application you have previously allowed to access the Internet has changed. If you have not recently upgraded the application in question, you should be careful about granting the modified application access to the Internet. (Trusting, Standard, or Tight Security)
- **Application Requests Server Access** — This alert appears when Personal Firewall detects that an application you have previously allowed to access the Internet has requested Internet access as a server. (Tight Security)

Green Alerts

Green alerts inform you of changes that have been made to Personal Firewall. For example, green alerts can inform you of applications to which Personal Firewall has automatically granted Internet Access, or inform you of any new application rules.

- **Program Allowed to Access the Internet** — This alert appears when Personal Firewall automatically grants Internet access for all new or modified applications, and then notifies you (Trusting Security). An example of a modified application is one with modified rules to automatically allow the application Internet access.

Blue Alerts

Blue alerts contain information, but require no response from you.

- **Connection Attempt Blocked** — This alert appears when Personal Firewall blocks unwanted Internet or network traffic. (Trusting, Standard, or Tight Security)

Connection Attempt Blocked

If you selected **Trusting, Standard,** or **Tight** security, Personal Firewall displays an alert (Figure 2-5) when it blocks unwanted Internet or network traffic.

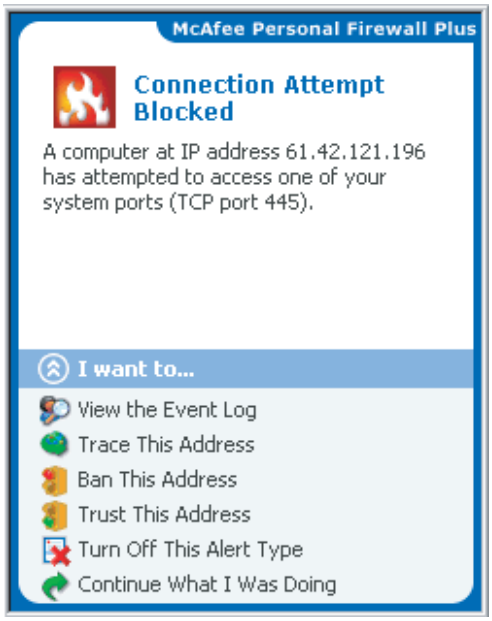

Figure 2-5. Connection Attempt Blocked alert

View a brief description of the event, then choose from these options:

- Click **View the Event Log** to get details about the event through the Personal Firewall Inbound Events log (see *About Inbound Events* on page 16 for details).
- Click **Trace This Address** to perform a Visual Trace of the IP addresses for this event.
- Click **Ban This Address** to block this address from accessing your computer. The address is added to the Banned IP Addresses list.
- Click **Trust This Address** to allow this IP address to access your computer.
- Click **Continue What I Was Doing** if you do not want to take action beyond what Personal Firewall has already done.

Internet Application Blocked!

If a Trojan program alert appears (Figure 2-6), Personal Firewall automatically denies this program access to the Internet and recommends that you scan your computer for viruses.

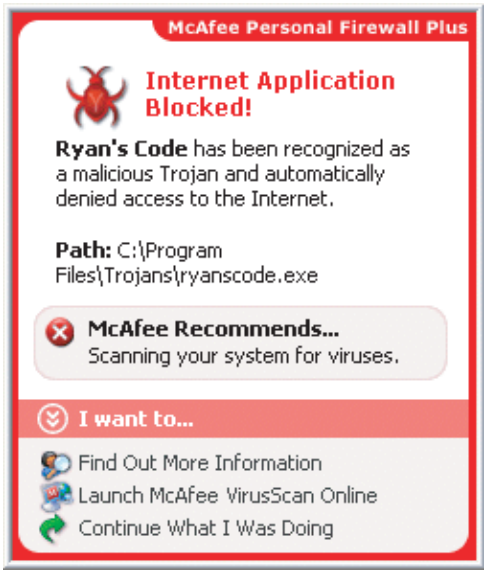

Figure 2-6. Internet Application Blocked alert

View a brief description of the event, then choose from these options:

- Click **Find Out More Information to get details** about the event through the Inbound Events log (see *About Inbound Events* on page 16 for details).
- Click **Launch McAfee VirusScan Online** to scan your computer for viruses.
- Click **Continue What I Was Doing** if you do not want to take action beyond what Personal Firewall has already done.

Application Wants to Access the Internet

If you selected **Standard** or **Tight** security in the Security Settings options, Personal Firewall displays an alert (Figure 2-7) when it detects Internet or network traffic for new or modified applications.

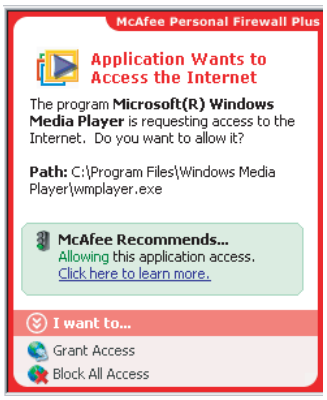

Figure 2-7. Application Wants to Access the Internet alert

If an alert appears recommending caution in allowing the application Internet access, you can click **Click here to learn more** to get more information about the application. This option appears on the alert only if Personal Firewall is configure to use Smart Recommendations.

McAfee might not recognize the application trying to gain Internet access (Figure 2-8).

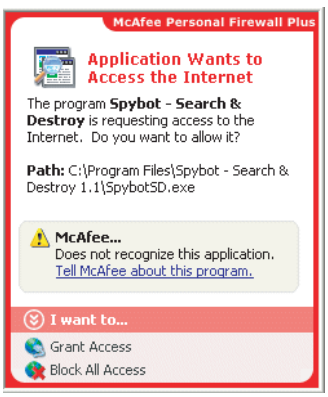

Figure 2-8. McAfee does not recognized this application alert

Therefore, McAfee cannot give you a recommendation on how to handle the application. You can report the application to McAfee by clicking **Tell McAfee about this program**. A web page appears and asks you for information related to the application. Please fill out as much information as you know.

The information you submit is used in conjunction with other research tools by our HackerWatch operators to determine whether an application warrants being listed in our known applications database, and if so, how it should be treated by Personal Firewall.

View a brief description of the event, then choose from these options:

- Click **Grant Access** to allow the application to both send data and receive unsolicited data on non-system ports.
- Click **Block All Access** to prevent the application from sending or receiving data.

IMPORTANT
You must grant access to applications that require Internet access for online product updates (such as McAfee Security services) to keep them up-to-date.

Application Has Been Modified

If you selected **Trusting, Standard**, or **Tight** security in the Security Settings options, Personal Firewall displays an alert (Figure 2-9) when Personal Firewall detects that an application you have previously allowed to access the Internet has changed. If you have not recently upgraded the application in question, be careful about granting the modified application access to the Internet.

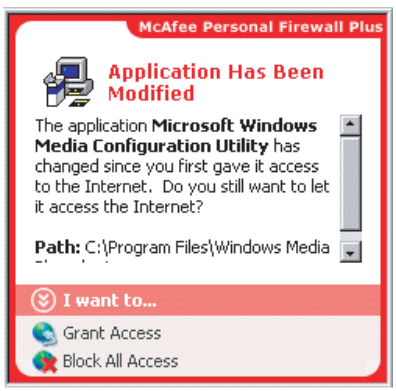

Figure 2-9. Application Has Been Modified alert

View a brief description of the event, then choose from these options:

- Click **Grant Access** to allow the application to both send data and receive unsolicited data on non-system ports.
- Click **Block All Access** to prevent the application from sending or receiving data.

Application Requests Server Access

If you selected **Tight** security in the Security Settings options, Personal Firewall displays an alert (Figure 2-10) when it detects that an application you have previously allowed to access the Internet has requested Internet access as a server.

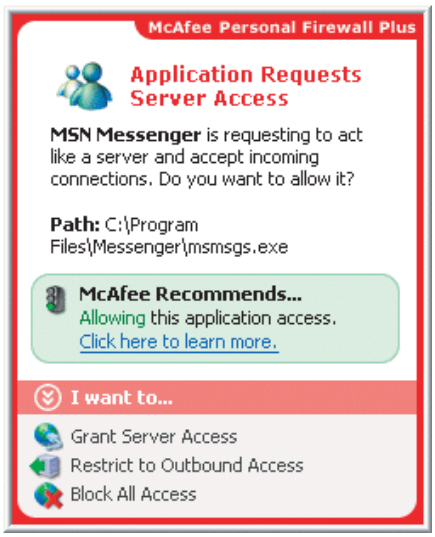

Figure 2-10. Application Requests Server Access alert

For example, an alert appears when MSN Messenger requests server access to send a file during a chat.

View a brief description of the event, then choose from these options:

- Click **Grant Server Access** to allow the application to both send and receive data.
- Click **Restrict to Outbound Access** to prevent the application from receiving data.
- Click **Block All Access** to prevent the application from sending or receiving data.

Program Allowed to Access the Internet

If you selected **Trusting** security in the Security Settings options, Personal Firewall automatically grants Internet access for all new or modified applications, then notifies you with an alert (Figure 2-11).

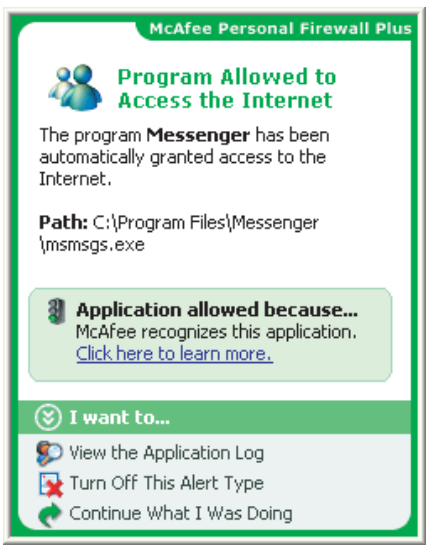

Figure 2-11. Program Allowed to Access the Internet

View a brief description of the event, then choose from these options:

- Click **View the Application Log** to get details about the event through the Internet Applications Log (see *About Internet Applications* on page 14 for details).
- Click **Turn Off This Alert Type** to prevent these types of alerts from appearing.
- Click **Continue What I Was Doing** if you do not want to take action beyond what Personal Firewall has already done.

A

alerts, 26
- Application Has Been Modified, 27
- Application Requests Internet Access, 27
- Application Requests Server Access, 27
- Connection Attempt Blocked, 27
- New Application Allowed, 27

D

downloading Personal Firewall, 7

E

Event Log
- about, 16
- managing, 24
- viewing, 25

events
- about, 16
- archiving the Event Log, 24
- clearing the Event Log, 25
- copying, 26
- deleting, 26
- exporting, 25
- from 0.0.0.0, 18
- from 127.0.0.1, 18
- from computers on your LAN, 19
- from private IP addresses, 19
- HackerWatch.org advice, 22
- loopback, 18
- more information, 22
- reporting, 22
- responding to, 21
- showing
  - all, 20
  - from one address, 21
  - one day's, 21
  - this week's, 20
  - today's, 20
  - with same event info, 21
- tracing
  - understanding, 16
  - viewing archived Event Logs, 25

G

getting started, 5

H

HackerWatch.org
- advice, 22
- reporting an event to, 22
- signing up, 22

I

installing Personal Firewall, 7

Internet applications
- about, 14
- changing applications, 16
- changing permissions, 15

IP addresses
- about, 17

M

McAfee SecurityCenter, 9

N

new features, 5

P

Personal Firewall
installing, 7
opening, 11
testing, 9
using, 11

R

reporting an event, 22

S

showing events in the Event Log, 20
Summary Page, 11
system requirements, 6

T

testing Personal Firewall, 9
tracing an event, 22

U

uninstalling
other firewalls, 7